

Het EPD en privacy

(Gepubliceerd in: Journaal Privacy Gezondheidszorg, nummer 7, augustus 2008, jaargang 9)

Mw. mr. M.J. Bonthuis¹

Inleiding

Patiëntgegevens, die op decentraal niveau bij de zorgverlener zijn opgeslagen, kunnen binnen het in ontwikkeling zijnde landelijk Elektronisch Patiëntendossier (EPD) van het ministerie van VWS voor alle zorgaanbieders beschikbaar worden gemaakt. Een landelijk EPD heeft een grote maatschappelijke betekenis, maar brengt ook aanzienlijke risico's met zich mee. Het ministerie van VWS beoogt een doelmatiger gebruik van de beschikbare informatie over patiënten, waarmee fouten en het doen van onnodig onderzoek voorkomen kunnen worden. Daarnaast levert de landelijke uitwisseling van gegevens een kostenbesparing op. Echter, er ontstaan risico's als het gaat om de vertrouwelijke omgang met de medische informatie door de verschillende zorgaanbieders. Daarnaast kunnen door de komst van het EPD steeds méér gegevens over patiënten worden verwerkt en uitgewisseld. Hierdoor staat de privacy van patiënten onder druk. Vanwege deze grootschaligheid is de vraag of door de komst van het EPD de vertrouwelijkheid tussen zorgverlener en patiënt en diens privacy op basis van de huidige wet- en regelgeving nog steeds gegarandeerd kan worden.

Het EPD

De structuur van het landelijk EPD bestaat uit een Landelijk Schakelpunt (LSP), de zogenaamde verkeerstoren, en een verwijfsindex (VI).

Het LSP fungeert als belangrijke speler in de landelijke structuur en controleert de rechtmatigheid van de toegang door middel van autorisatie op basis van het functieprofiel van de zorgverlener. Daarnaast kan de patiënt door het geven van toestemming aan zorgverleners toegang tot zijn dossier geven. De patiënt kan ook bezwaar maken tegen verstrekking aan bepaalde zorgverleners. Dit alles wordt opgenomen in een zogenaamd autorisatieprotocol. De verwijfsindex (VI) die gebruikt wordt door de zorgverlener zorgt voor een doelmatige zoekmethode door eerst te tonen *waar* de gegevens zich bevinden zonder deze direct zichtbaar te maken. Door een logfile is achteraf te controleren wie inzage heeft gehad en of deze rechtmatig is geweest. Het is belangrijk dat er vooraf te bepalen is wie er toegang tot de gegevens heeft, ook wel authenticatie genoemd. De zorgverlener identificeert en authenticceert zichzelf door middel van de Unieke Zorgverleners Identificatie (UZI)-pas. De patiënt doet dat op basis van zijn Burger Service Nummer (BSN).

Om aan te kunnen sluiten op het LSP zullen de zorginstellingen moeten voldoen aan de eisen van een Goed Beheerd Zorgsysteem (GBZ). Daarnaast zal het datacommunicatienetwerk waarover de uitwisseling plaatsvindt gekwalificeerd moeten zijn als Zorg Service Provider (ZSP).

Het EPD kent een aantal hoofdstukken die gefaseerd in worden gevoerd. Het ministerie start met de uitrol van het Waarneemdossier Huisartsen (WDH) en het Elektronisch Medicatiedossier (EMD). Het Elektronisch Laboratoriumdossier (e-Lab), het Elektronisch Kinddossier (EKD) en het e-Diabetesdossier zullen in de toekomst volgen. De bedoeling is dat op 1 januari 2009 50% van de zorgaanbieders aangesloten is op het LSP.

¹ M.J. Bonthuis is IT-Jurist bij IT's Privacy met als specialisatie de implementatie van de WBP. Met haar scriptie over Privacy en het landelijke EPD won zij in 2008 de landelijke Privacy Scriptieprijs van de Stichting Privacy en Registratie.

Vertrouwelijkheid en het EPD

Goede zorgverlening valt of staat met correcte en volledige informatie over de patiënt. De vertrouwelijke omgang met de patiëntgegevens is daarbij echter van essentieel belang. De patiënt moet kunnen rekenen op een verantwoorde omgang met zijn, grotendeels gevoelige, gegevens. De patiënt zou immers niet onverkort alles aan de zorgverlener meedelen wanneer de geheimhouding daarvan niet kan worden gegarandeerd. De gegevens kunnen dan opduiken in situaties waarin dat niet wenselijk is.

Het fundament uit het gezondheidsrecht dat tegemoet komt aan de vertrouwelijke omgang met patiënt gegevens, is het beroepsgeheim uit de Wet Geneeskundige Behandelingsovereenkomst (WGBö). Het beroepsgeheim (als recht van de patiënt) bestaat uit een zwijgplicht en een verschoningsrecht. De zwijgplicht betekent voor de zorgverlener dat zonder (schriftelijke) toestemming geen informatie mag worden verstrekt aan anderen dan de patiënt. Het verschoningsrecht is het recht van de zorgverlener om te zwijgen tegenover een rechter. Het beroepsgeheim kan slechts in bepaalde gevallen en om vooraf bepaalde (zwaarwegende) redenen worden doorbroken. Het betreft dan situaties waarin de verstrekking plaats vindt binnen het behandelteam of indien er sprake is van een conflict van plichten. De WGBö heeft met name als doel het versterken van de positie van de patiënt. Naast de verplichte geheimhouding van de verstrekte informatie stelt de WGBö eisen ten aanzien van de zorgverlener en het opstellen van een (medisch) dossier.

Het juridisch kader en het EPD (WGBö en WBP)

Het juridisch kader is onverkort van toepassing op het EPD.

Echter, door de komst van het EPD zal de invulling van de begrippen uit de WGBö en de WBP veranderen en zullen we zien dat deze worden opgerekt. Dit geldt met name voor wat betreft de toegang op basis van de behandelrelatie.

Tot voor kort was de behandelrelatie als mogelijke doorbreking van het beroepsgeheim niet opgenomen binnen de autorisatiestructuur van het EPD. Dat lijkt nu echter wel het geval te zijn. Op 9 mei 2008 stemde de ministerraad immers in met het wetsvoorstel, dat regelt dat in beginsel alleen de beroepsbeoefenaar die een behandelrelatie met een patiënt heeft, toegang krijgt tot diens medisch dossier.² Bij het aangaan van een behandelrelatie met een nieuwe patiënt zal de zorgverlener expliciet aan het systeem (door middel van het plaatsen van een vinkje) moeten aangeven dat hij een behandelrelatie heeft. De rechtmatigheid wordt achteraf door middel van een logfile gecontroleerd. Het pas achteraf controleren is gezien de WGBö niet toelaatbaar en kan dan ook als een uitholling van het beroepsgeheim worden aangemerkt. De vraag die daarnaast rijst, is hoe intensief de controle op rechtmatige toegang op die schaal mogelijk is.

Voor een bestaande behandelrelatie stelt de minister dat uit de (financiële) administratie de behandelrelatie zou moeten blijken. Echter, de behandelrelatie is niet altijd terug te voeren op historische gegevens. Het uitwisselen van patiëntinformatie binnen het behandelteam zal in de praktijk vaak afhankelijk zijn van de beschikbaarheid binnen de gekozen zorginstelling en/of de keuze van de patiënt. Welke medebehandelaars door die hoofdbehandelaar zullen worden betrokken bij de behandeling is ook sterk afhankelijk van hun beschikbaarheid op dat moment. Vaak is er geen tijd om de precieze betrokkenheid van iedere medebehandelaar vast te leggen. In principe mag een hoofdbehandelaar zonder toestemming van de patiënt een medebehandelaar en medewerker toegang tot diens gegevens verlenen, maar in de praktijk is moeilijk *per geval* vast te leggen wie dat precies zijn. Ook als zorgverleners *vooraf* aangeven

² CBP 15-5-2008:

http://www.cbpweb.nl/documenten/pb_20080428_toegang_epd.shtml?refer=true&theme=purple

welke collega's ooit als medebehandelaar of medewerker zullen optreden, biedt dit geen sluitende oplossing.³

Om uitwisseling van patiëntgegevens tussen zorgverleners praktisch mogelijk te maken zou de patiënt generiek en van tevoren toestemming moeten geven. We zien dat de doorbreking van het beroepsgeheim op basis van deze toestemming evenzeer wordt opgerekt. Het gebruik van de vooraf gegeven generieke toestemming door de patiënt is geen passende methode voor het ontsluiten van medische gegevens en kan een containerbegrip worden. Tevens past het niet binnen de reikwijdte van de noodzakelijkheidseis uit de WGBa, dat stelt dat niet meer gegevens mogen worden verwerkt dan strikt noodzakelijk zijn voor de behandeling van de patiënt.

De patiënt heeft weliswaar de mogelijkheid om bezwaar te maken tegen bepaalde uitwisselingen, maar dat is lastig van tevoren te bepalen. Welke zorgverlener de behandelrelatie met een patiënt aangaat, is vaak afhankelijk van de beschikbaarheid binnen de gekozen zorginstelling en/of de keuze van de patiënt. Vaak is er geen tijd om de precieze betrokkenheid van iedere medebehandelaar vast te leggen. Daarbij komt dat per zorgverlener de rol waarin hij de gegevens opvraagt per geval kan verschillen.

De huidige dossiers zijn niet of niet goed geschikt voor selectieve informatie-uitwisseling.⁴ Het gebruik van digitale dossiers vormt daarnaast een risico met name als het gaat om het verwijderen van gegevens. Het vernietigen van een papieren dossier is vrij eenvoudig. Het vernietigen van een digitaal dossier niet. Er is immers niet te garanderen dat alle aftreksels of back-ups zijn verwijderd. Het kan dus voorkomen, dat, als gevolg van het verstrijken van de bewaartermijn of op verzoek van de patiënt, de gegevens zijn verwijderd, terwijl deze nog op allerlei plaatsen (digitaal of op papier) kunnen "opduiken".

Naast de bepalingen uit de WGBa bepaalt de WBP vervolgens de eisen ten aanzien van verwerkingen van persoonsgegevens en is dan ook een belangrijk normatief kader voor de uitwisseling van patiëntinformatie binnen het EPD. Het College Bescherming Persoonsgegevens (CBP), dat toezicht houdt op de naleving van de WBP, heeft ten aanzien van het EPD een aantal stellingen ingenomen. Ten eerste onderschrijft het CBP dat het belang én het succes van een EPD afhankelijk is van het feit of het systeem vertrouwelijk omgaat met de patiëntgegevens. De toegang tot het EPD zal dan ook in overeenstemming moeten zijn met het hoofddoel van het EPD. Maar de meeste zorg wordt door het CBP uitgesproken over het toezicht, dat passend en met voldoende waarborgen omkleed dient te zijn. Ook door patiënten wordt dit als belangrijk ervaren. Daardoor veronderstelt de nieuwe werkwijze een aanzienlijke aanpassing als het gaat om (het bewustzijn omtrent) de beveiliging van de gevoelige gegevens. Gezien de omvang, complexiteit en de risico's van het EPD kan dan ook niet met een algemeen toezicht worden volstaan. Er kunnen immers ingewikkelde situaties ontstaan doordat verschillende toezichthoudende organen vanuit hun eigen perspectief naar de verwerking kijken, terwijl een overkoepelende blik noodzakelijk is. Het CBP en de Inspectie voor de Gezondheidszorg hebben aangegeven dat zij de toezichthoudende activiteiten van het EPD niet kunnen uitvoeren. Mede door de complexiteit en de nieuwe risico's pleit het CBP er dan ook voor het toezicht te onderwerpen aan een specifiek voor dat doel op te richten autoriteit.

Conclusie

3 J. Beuving, Mag een zorgverlener die naast je woont vrij opzoeken wat je mankeert? Volkskrant, 16 juni 2007.

4 Richtlijn inzake omgaan met medische gegevens, KNMG: Utrecht 2004

We zien dat de begrippen uit de WGBo en de WBP veranderen in de nieuwe context van het EPD. Naast de problemen die de invoering van het EPD binnen het bestaande begrippenkader ondervindt, is tevens sprake van enkele nieuwe risico's die met de komst van een EPD gepaard gaan. Ten eerste kan gedacht worden aan het ontstaan van risico's door gegevens op grote schaal te digitaliseren. Zo blijkt uit de praktijk dat de stap van papieren naar digitale dossiers op lokaal niveau al de nodige problemen oplevert en hier wordt op landelijk niveau nog onvoldoende rekening mee gehouden.⁵ Door toenemende digitalisering van gegevens -en door de invoering van een EPD neemt dit nog verder toe en kunnen er op het gebied van de privacy grotere risico's ontstaan. Met name in een elektronische omgeving zijn deze regels van belang, gezien het vergrote risico op privacyschade door de mogelijkheid van een lek in het EPD. Digitaal beschikbare gegevens zijn immers makkelijker en op grotere schaal te verspreiden. Ook in de zorg maken vorderingen van informatietechnologieën de verwerking en uitwisseling van gegevens aanzienlijk makkelijker. Uiteraard is voor zorgaanbieders een hoge bruikbaarheid gewenst, maar de keuze voor de bruikbaarheid mag niet inhouden dat het beschermingsniveau daardoor lager wordt.

In het kader van de aansprakelijkheid is aandacht voor de bewijspositie, wanneer niet geheel duidelijk is of een opvrager kan aantonen welke concrete medische gegevens hij wel of niet heeft ontvangen, essentieel. Het is nog maar de vraag waar de verantwoordelijkheid ligt voor het niet opnemen/ ontvangen van belangrijke gegevens die wel ontvangen/ opgenomen hadden moeten zijn.

Mede vanwege de impact op patiënten en de behoefte aan transparantie zal één en ander in een alomvattend juridisch kader gegoten moeten worden. Speciale waarborgen van patiënten zullen daarin gegarandeerd moeten worden.

⁵ ICT in ziekenhuizen, beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg, IGZ: Utrecht 2004 en Preoperatief traject ontbeert multidisciplinaire en gestandaardiseerde aanpak en teamvorming, IGZ: Utrecht 2007.